【書類名】　特許願

【整理番号】　A009904769

【提出日】　平成11年 8月31日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F　7/00

【発明の名称】　拡大鍵生成装置、暗復号装置及び記憶媒体

【請求項の数】　20

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　大森　基司

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　横田　薫

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　関部　勉

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　館林　誠

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　佐野　文彦

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　川村　信一

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705037

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　拡大鍵生成装置、暗復号装置及び記憶媒体

【特許請求の範囲】

【請求項１】　各ラウンド毎に異なる鍵が入力され、それぞれ前記鍵に基づいて拡大鍵を生成する複数の鍵変換関数部がカスケードに連結された拡大鍵生成装置であって、

前記各鍵変換関数部は、

前記入力された鍵から得られた第１鍵に基づいて所定の置換テーブルにより変換処理を行う第１鍵変換手段と、

この第１鍵変換手段による変換結果と前記入力された鍵から得られた第２鍵とに基づいて前記拡大鍵を算出する拡大鍵算出手段と

を備えたことを特徴とする拡大鍵生成装置。

【請求項２】　請求項１に記載の拡大鍵生成装置において、

前記各鍵変換関数部は、

入力された鍵を左又は右に巡回シフトさせ、前記巡回シフトの完了した鍵を次ラウンドの鍵変換関数部に入力する巡回シフト手段を備えたことを特徴とする拡大鍵生成装置。

【請求項３】　請求項２に記載の拡大鍵生成装置において、

前記巡回シフト手段のシフト量は、前記第１鍵変換手段の出力ビット数と互いに素な値であることを特徴とする拡大鍵生成装置。

【請求項４】　請求項１に記載の拡大鍵生成装置において、

前記各鍵変換関数部は、

入力された鍵を置換テーブルにより変換し、この変換の完了した鍵を次ラウンドの鍵変換関数部に入力する入力鍵変換手段を備えたことを特徴とする拡大鍵生成装置。

【請求項５】　請求項１乃至請求項４のいずれか１項に記載の拡大鍵生成装置において、

前記各鍵変換関数部は、

前記第１鍵変換手段による変換結果を拡大変換させて前記拡大鍵算出手段に入

力する拡大変換手段を備えたことを特徴とする拡大鍵生成装置。

【請求項６】　請求項５に記載の拡大鍵生成装置において、

前記拡大変換手段による拡大変換は、所定ビット数のシフトであることを特徴とする拡大鍵生成装置。

【請求項７】　請求項１乃至請求項６のいずれか１項に記載の拡大鍵生成装置において、

前記拡大鍵演算手段による演算は、桁上りを伴う加算であることを特徴とする拡大鍵生成装置。

【請求項８】　請求項１乃至請求項７のいずれか１項に記載の拡大鍵生成装置を備えた暗復号装置において、

前記各鍵変換関数部により生成された各拡大鍵に基づいて、入力された平文を暗号化して暗号文を出力し、且つ、入力された暗号文を復号して平文を出力する攪拌部を備えたことを特徴とする暗復号装置。

【請求項９】　請求項８に記載の暗復号装置において、

前記攪拌部は、前記暗号化及び前記復号のための複数の置換テーブルを有し、

前記攪拌部のいずれかの置換テーブルは、前記第１鍵変換手段の置換テーブルと共有化されていることを特徴とする暗復号装置。

【請求項１０】　請求項９に記載の暗復号装置において、

前記各鍵変換関数部は、

前記第１鍵変換手段による変換結果を受けたとき、この変換結果のビット数の半分のビット数、あるいは前記半分のビット数に前記変換結果のビット数の整数倍を加えた値のビット数だけ、当該変換結果を左シフトさせて前記拡大鍵算出手段に入力する拡大変換手段を備えたことを特徴とする暗復号装置。

【請求項１１】　各ラウンド毎に異なる鍵が入力され、それぞれ前記鍵に基づいて拡大鍵を生成する複数の鍵変換関数部がカスケードに連結された拡大鍵生成装置に使用されるコンピュータ読み取り可能な記憶媒体であって、

前記拡大鍵生成装置内のコンピュータに、

前記各鍵変換関数部として、

前記入力された鍵から得られた第１鍵に基づいて所定の置換テーブルにより変

換処理を行う第１鍵変換手段、

この第１鍵変換手段による変換結果と前記入力された鍵から得られた第２鍵とに基づいて前記拡大鍵を算出する拡大鍵算出手段、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項１２】　請求項１１に記載のコンピュータ読み取り可能な記憶媒体において、

前記各鍵変換関数部としては、

入力された鍵を左又は右に巡回シフトさせ、前記巡回シフトの完了した鍵を次ラウンドの鍵変換関数部に入力する巡回シフト手段、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項１３】　請求項１２に記載のコンピュータ読み取り可能な記憶媒体において、

前記巡回シフト手段のシフト量は、前記第１鍵変換手段の出力ビット数と互いに素な値であるコンピュータ読み取り可能な記憶媒体。

【請求項１４】　請求項１１に記載のコンピュータ読み取り可能な記憶媒体において、

前記各鍵変換関数部としては、

入力された鍵を置換テーブルにより変換し、この変換の完了した鍵を次ラウンドの鍵変換関数部に入力する入力鍵変換手段、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項１５】　請求項１１乃至請求項１４のいずれか１項に記載のコンピュータ読み取り可能な記憶媒体において、

前記各鍵変換関数部としては、

前記第１鍵変換手段による変換結果を拡大変換させて前記拡大鍵算出手段に入力する拡大変換手段、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒

体。

【請求項１６】　請求項１５に記載のコンピュータ読み取り可能な記憶媒体において、

前記拡大変換手段による拡大変換は、所定ビット数のシフトであるコンピュータ読み取り可能な記憶媒体。

【請求項１７】　請求項１１乃至請求項１６のいずれか１項に記載のコンピュータ読み取り可能な記憶媒体において、

前記拡大鍵演算手段による演算は、桁上りを伴う加算であるコンピュータ読み取り可能な記憶媒体。

【請求項１８】　請求項１１乃至請求項１７のいずれか１項に記載の拡大鍵生成装置を備えた暗復号装置に使用されるコンピュータ読み取り可能な記憶媒体において、

前記暗復号装置内のコンピュータに、

前記各鍵変換関数部により生成された各拡大鍵に基づいて、入力された平文を暗号化して暗号文を出力し、且つ、入力された暗号文を復号して平文を出力する攪拌部、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項１９】　請求項１８に記載のコンピュータ読み取り可能な記憶媒体において、

前記攪拌部は、前記暗号化及び前記復号のための複数の置換テーブルを有し、

前記攪拌部のいずれかの置換テーブルは、前記第１鍵変換手段の置換テーブルと共有化されているコンピュータ読み取り可能な記憶媒体。

【請求項２０】　請求項１９に記載のコンピュータ読み取り可能な記憶媒体において、

前記各鍵変換関数部としては、

前記第１鍵変換手段による変換結果を受けたとき、この変換結果のビット数の半分のビット数、あるいは前記半分のビット数に前記変換結果のビット数の整数倍を加えた値のビット数だけ、当該変換結果を左シフトさせて前記拡大鍵算出手

段に入力する拡大変換手段、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、秘密鍵ブロック暗号に適用される拡大鍵生成装置、暗復号装置及び記憶媒体に関する。

【０００２】

【従来の技術】

近年の計算機・通信技術の分野では、送信データを暗号化して送信し、受信データを復号して受信内容を得る暗号技術が広く知られている。この種の暗号技術では、暗号化と復号に同じ秘密鍵（以下、共通鍵という）を用いる暗号化アルゴリズムが共通鍵暗号と呼ばれている。共通鍵暗号では、一般に、入力メッセージが固定長の入力ブロックに分割され、各ブロックが鍵に基づいて攪拌処理され、暗号文が生成されている。係る共通鍵暗号としては、例えばＤＥＳ（データ暗号化規格：data encryption standard）と呼ばれる方式が広く用いられている。

【０００３】

ＤＥＳ方式による暗号化では、図１５（ａ）に示すように、平文に初期転置ＩＰを施したデータに対し、ラウンド関数による処理を１６回施す。さらにラウンド関数処理されたデータに初期転置の逆転置$ＩＰ^{-1}$を施すことで暗号文を得ている。また、各ラウンド関数に対し、元の鍵から生成される拡大鍵を与えることでラウンド関数における処理が実行される。

【０００４】

つまり、ＤＥＳ方式による暗号化装置は、多数のラウンド関数によって暗号化対象となるデータを攪拌する攪拌部と、攪拌部の各ラウンド関数に拡大鍵を与える鍵生成部をその主要構成としている。

【０００５】

一方、ＤＥＳ方式による復号は、図１５（ｂ）に示すように、暗号化時とは逆

の順番で復号対象のデータにラウンド関数の処理を施す。従って、鍵生成部からの拡大鍵も、暗号化時の最後のラウンド関数で使用されたものから順番に生成する。

【０００６】

このＤＥＳ方式における第１の利点は、暗号化回路と復号回路の大半を共通化可能な構成にある。つまり、図１５（ａ），図１５（ｂ）に示すように、攪拌部のラウンド関数は、暗号化時と復号時とでは拡大鍵の入力順序は逆になるが、同一の回路が使用される。

【０００７】

ＤＥＳ方式の第２の利点は、１つの共通鍵を用いて暗号化と復号とを行うため、管理対象の鍵が少ないことである。なお、ＤＥＳ方式では、唯一の共通鍵に基づいて拡大鍵を逆順に生成するため、鍵生成部では次の処理を行っている。

【０００８】

すなわち、暗号化の際には、共通鍵を左巡回シフト（左ローテート）し、各拡大鍵を生成する。なお、巡回シフト量の合計値を共通鍵のビット数に定め、最終段で中間的な鍵が初期状態（共通鍵）に戻される。これにより、暗号化時の最後の拡大鍵と復号時の最初の拡大鍵とを同一の値に生成し得る。復号時には、共通鍵を逆に右巡回シフト（右ローテート）して逆順に各拡大鍵を生成すればよい。

【０００９】

しかしながら、ＤＥＳ方式では、鍵生成部の処理が転置処理のみで構成されるため、一般に弱鍵（weak key）と呼ばれる安全性の低い鍵が存在するという問題がある。なお、弱鍵は、本明細書中、互いに同一な拡大鍵を意味しており、全ての拡大鍵Ｋ１～Ｋ１６が互いに同一な場合（Ｋ１＝Ｋ２＝…＝Ｋ１６）と、半分の拡大鍵Ｋ１～Ｋ８，Ｋ９～Ｋ１６が互いに同一な場合（Ｋ１＝Ｋ１６，Ｋ２＝Ｋ１５，…，Ｋ８＝Ｋ９）とを含んでいる。

【００１０】

但し、係る弱鍵の生成は、脅威的なものではなく、弱鍵を生成するパターンをもつ共通鍵の入力を除去する装置、あるいは生成された拡大鍵が弱鍵でないか否かを判別し且つ弱鍵のときには除去する装置を付加することにより、充分に阻止

可能であると考えられる。

【００１１】

しかしながら、この種の弱鍵の生成阻止に関する装置を付加した場合、拡大鍵生成装置及び暗復号装置の価格を上昇させてしまい、さらに、拡大鍵生成装置及び暗復号装置の規模を増大させる可能性がある。

【００１２】

また、ＤＥＳ方式に限らず、弱鍵の生成を阻止することにより、本来の各ラウンド毎に異なる拡大鍵を用いた場合の暗号強度を実現させ、さらに、その暗号強度を向上し得る暗号方式が望まれている。

【００１３】

【発明が解決しようとする課題】

以上説明したように従来の拡大鍵生成装置及び暗復号装置では、安全性の低下を阻止する観点から、弱鍵の生成阻止に関する装置を付加すると、拡大鍵生成装置及び暗復号装置の価格を上昇させてしまい、さらに、拡大鍵生成装置及び暗復号装置の規模を増大させる可能性がある。

【００１４】

また、弱鍵の生成を阻止しても、鍵生成部の処理が暗号強度の向上にあまり貢献しておらず、暗号強度の向上が望まれている。

【００１５】

本発明は上記実情を考慮してなされたもので、装置価格や装置規模を抑え、弱鍵の生成を阻止しつつ拡大鍵の攪拌性を向上でき、もって、暗号強度の向上を図り得る拡大鍵生成装置、暗復号装置及び記憶媒体を提供することを目的とする。

【００１６】

【課題を解決するための手段】

請求項１に対応する発明は、各ラウンド毎に異なる鍵が入力され、それぞれ前記鍵に基づいて拡大鍵を生成する複数の鍵変換関数部がカスケードに連結された拡大鍵生成装置であって、前記各鍵変換関数部としては、前記入力された鍵から得られた第１鍵に基づいて所定の置換テーブルにより変換処理を行う第１鍵変換手段と、この第１鍵変換手段による変換結果と前記入力された鍵から得られた第

２鍵とに基づいて前記拡大鍵を算出する拡大鍵算出手段とを備えた拡大鍵生成装置である。

【００１７】

また、請求項２に対応する発明は、請求項１に対応する拡大鍵生成装置において、前記各鍵変換関数部としては、入力された鍵を左又は右に巡回シフトさせ、前記巡回シフトの完了した鍵を次ラウンドの鍵変換関数部に入力する巡回シフト手段を備えた拡大鍵生成装置である。

【００１８】

さらに、請求項３に対応する発明は、請求項２に対応する拡大鍵生成装置において、前記巡回シフト手段のシフト量としては、前記第１鍵変換手段の出力ビット数と互いに素な値である拡大鍵生成装置である。

【００１９】

また、請求項４に対応する発明は、請求項１に対応する拡大鍵生成装置において、前記各鍵変換関数部としては、入力された鍵を置換テーブルにより変換し、この変換の完了した鍵を次ラウンドの鍵変換関数部に入力する入力鍵変換手段を備えた拡大鍵生成装置である。

【００２０】

さらに、請求項５に対応する発明は、請求項１乃至請求項４のいずれか１項に対応する拡大鍵生成装置において、前記各鍵変換関数部としては、前記第１鍵変換手段による変換結果を拡大変換させて前記拡大鍵算出手段に入力する拡大変換手段を備えた拡大鍵生成装置である。

【００２１】

また、請求項６に対応する発明は、請求項５に対応する拡大鍵生成装置において、前記拡大変換手段による拡大変換としては、所定ビット数のシフトである拡大鍵生成装置である。

【００２２】

さらに、請求項７に対応する発明は、請求項１乃至請求項６のいずれか１項に対応する拡大鍵生成装置において、前記拡大鍵演算手段による演算としては、桁上りを伴う加算である拡大鍵生成装置である。

【００２３】

また、請求項８に対応する発明は、請求項１乃至請求項７のいずれか１項に対応する拡大鍵生成装置を備えた暗復号装置において、前記各鍵変換関数部により生成された各拡大鍵に基づいて、入力された平文を暗号化して暗号文を出力し、且つ、入力された暗号文を復号して平文を出力する攪拌部を備えた暗復号装置である。

【００２４】

さらに、請求項９に対応する発明は、請求項８に対応する暗復号装置において、前記攪拌部が、前記暗号化及び前記復号のための複数の置換テーブルを有し、前記攪拌部のいずれかの置換テーブルが、前記第１鍵変換手段の置換テーブルと共有化されている暗復号装置である。

【００２５】

また、請求項１０に対応する発明は、請求項９に対応する暗復号装置において、前記各鍵変換関数部としては、前記第１鍵変換手段による変換結果を受けたとき、この変換結果のビット数の半分のビット数、あるいは前記半分のビット数に前記変換結果のビット数の整数倍を加えた値のビット数だけ、当該変換結果を左シフトさせて前記拡大鍵算出手段に入力する拡大変換手段を備えた暗復号装置である。

【００２６】

さらに、請求項１１に対応する発明は、各ラウンド毎に異なる鍵が入力され、それぞれ前記鍵に基づいて拡大鍵を生成する複数の鍵変換関数部がカスケードに連結された拡大鍵生成装置に使用されるコンピュータ読み取り可能な記憶媒体であって、前記拡大鍵生成装置内のコンピュータに、前記各鍵変換関数部として、前記入力された鍵から得られた第１鍵に基づいて所定の置換テーブルにより変換処理を行う第１鍵変換手段、この第１鍵変換手段による変換結果と前記入力された鍵から得られた第２鍵とに基づいて前記拡大鍵を算出する拡大鍵算出手段、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【００２７】

また、請求項１２に対応する発明は、請求項１１に対応するコンピュータ読み取り可能な記憶媒体において、前記各鍵変換関数部としては、入力された鍵を左又は右に巡回シフトさせ、前記巡回シフトの完了した鍵を次ラウンドの鍵変換関数部に入力する巡回シフト手段、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【００２８】

さらに、請求項１３に対応する発明は、請求項１２に対応するコンピュータ読み取り可能な記憶媒体において、前記巡回シフト手段のシフト量が、前記第１鍵変換手段の出力ビット数と互いに素な値であるコンピュータ読み取り可能な記憶媒体である。

【００２９】

また、請求項１４に対応する発明は、請求項１１に対応するコンピュータ読み取り可能な記憶媒体において、前記各鍵変換関数部としては、入力された鍵を置換テーブルにより変換し、この変換の完了した鍵を次ラウンドの鍵変換関数部に入力する入力鍵変換手段、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【００３０】

さらに、請求項１５に対応する発明は、請求項１１乃至請求項１４のいずれか１項に対応するコンピュータ読み取り可能な記憶媒体において、前記各鍵変換関数部としては、前記第１鍵変換手段による変換結果を拡大変換させて前記拡大鍵算出手段に入力する拡大変換手段、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【００３１】

また、請求項１６に対応する発明は、請求項１５に対応するコンピュータ読み取り可能な記憶媒体において、前記拡大変換手段による拡大変換としては、所定ビット数のシフトであるコンピュータ読み取り可能な記憶媒体である。

【００３２】

さらに、請求項１７に対応する発明は、請求項１１乃至請求項１６のいずれか１項に対応するコンピュータ読み取り可能な記憶媒体において、前記拡大鍵演算

手段による演算が、桁上りを伴う加算であるコンピュータ読み取り可能な記憶媒体である。

【００３３】

また、請求項１８に対応する発明は、請求項１１乃至請求項１７のいずれか１項に対応する拡大鍵生成装置を備えた暗復号装置に使用されるコンピュータ読み取り可能な記憶媒体において、前記暗復号装置内のコンピュータに、前記各鍵変換関数部により生成された各拡大鍵に基づいて、入力された平文を暗号化して暗号文を出力し、且つ、入力された暗号文を復号して平文を出力する攪拌部、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【００３４】

さらに、請求項１９に対応する発明は、請求項１８に対応するコンピュータ読み取り可能な記憶媒体において、前記攪拌部が、前記暗号化及び前記復号のための複数の置換テーブルを有し、前記攪拌部のいずれかの置換テーブルが、前記第１鍵変換手段の置換テーブルと共有化されているコンピュータ読み取り可能な記憶媒体である。

【００３５】

また、請求項２０に対応する発明は、請求項１９に対応するコンピュータ読み取り可能な記憶媒体において、前記各鍵変換関数部としては、前記第１鍵変換手段による変換結果を受けたとき、この変換結果のビット数の半分のビット数、あるいは前記半分のビット数に前記変換結果のビット数の整数倍を加えた値のビット数だけ、当該変換結果を左シフトさせて前記拡大鍵算出手段に入力する拡大変換手段、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【００３６】

（作用）

従って、請求項１，１１に対応する発明は以上のような手段を講じたことにより、各鍵変換関数部としては、第１鍵変換手段が、入力された鍵から得られた第１鍵に基づいて所定の置換テーブルにより変換処理を行い、拡大鍵算出手段が、

この第１鍵変換手段による変換結果と入力された鍵から得られた第２鍵とに基づいて拡大鍵を算出する。

【００３７】

このように、外部装置を付加しない簡易な構成を用いており、拡大鍵を生成する際に、置換テーブルによる非線形変換処理を行うため、装置価格や装置規模を抑え、弱鍵の生成を阻止しつつ拡大鍵の攪拌性を向上でき、もって、暗号強度を向上させることができる。

【００３８】

また、請求項２，１２に対応する発明は、各鍵変換関数部としては、巡回シフト手段が、入力された鍵を左又は右に巡回シフトさせ、巡回シフトの完了した鍵を次ラウンドの鍵変換関数部に入力するので、請求項１，１１に対応する作用に加え、容易且つ確実に、各ラウンドに入力される鍵を互いに相違させることができる。

【００３９】

さらに、請求項３，１３に対応する発明は、巡回シフト手段のシフト量としては、第１鍵変換手段の出力ビット数と互いに素な値であるので、各ラウンドにおけるほぼ全ての第１鍵を互いに相違させることができ、請求項２，１２に対応する作用をより一層、容易且つ確実に奏することができる。

【００４０】

また、請求項４，１４に対応する発明は、各鍵変換関数部としては、入力鍵変換手段が、入力された鍵を置換テーブルにより変換し、この変換の完了した鍵を次ラウンドの鍵変換関数部に入力するので、請求項１，１１に対応する作用に加え、容易且つ確実に、各ラウンドに入力される鍵を互いに相違させることができる。

【００４１】

さらに、請求項５，１５に対応する発明は、各鍵変換関数部としては、拡大変換手段が、第１鍵変換手段による変換結果を拡大変換させて拡大鍵算出手段に入力するので、請求項１～４，１１～１４のいずれかに対応する作用に加え、第１鍵の攪拌作用を拡大鍵の任意の領域に反映させることができる。

【００４２】

また、請求項６，１６に対応する発明は、拡大変換手段による拡大変換としては、所定ビット数のシフトであるので、請求項５，１５に対応する作用を容易且つ確実に奏することができる。

【００４３】

さらに、請求項７，１７に対応する発明は、拡大鍵演算手段による演算としては、桁上りを伴う加算であるので、請求項１～６，１１～１６のいずれかに対応する作用を、容易且つ確実に奏することができる。

【００４４】

また、請求項８，１８に対応する発明は、攪拌部が、各鍵変換関数部により生成された各拡大鍵に基づいて、入力された平文を暗号化して暗号文を出力し、且つ、入力された暗号文を復号して平文を出力するので、請求項１～７，１１～１７のいずれかに対応する拡大鍵生成装置を備えた暗復号装置を実現することができる。

【００４５】

さらに、請求項９，１９に対応する発明は、攪拌部が、暗号化及び復号のための複数の置換テーブルを有し、攪拌部のいずれかの置換テーブルが、第１鍵変換手段の置換テーブルと共有化されているので、請求項８，１８に対応する作用に加え、装置規模の縮小化を図ることができる。

【００４６】

また、請求項１０，２０に対応する発明は、各鍵変換関数部としては、拡大変換手段が、第１鍵変換手段による変換結果を受けたとき、この変換結果のビット数の半分のビット数、あるいは半分のビット数に変換結果のビット数の整数倍を加えた値のビット数だけ、当該変換結果を左シフトさせて拡大鍵算出手段に入力するので、請求項９，１９に対応する作用に加え、第１鍵の攪拌作用を拡大鍵にて左シフトさせた領域に反映させることができ、この場合、攪拌部の複数の置換テーブルに入力される領域に反映させることができるので、より一層、暗号強度の向上を図ることができる。

【００４７】

【発明の実施の形態】

以下、本発明の各実施形態について図面を参照して説明する。

【００４８】

（第１の実施形態）

図１は本発明の第１の実施形態に係る暗復号装置の構成を示すブロック図であり、図２はこの暗復号装置内の拡大鍵生成部の構成を示すブロック図である。

【００４９】

この暗復号装置は、パーソナルコンピュータやワークステーション等の計算機の暗復号処理部として構成されており、ハードウェア又はソフトウェアによって暗号化処理と復号処理を行うものであって、具体的には、共通鍵からｎ段の拡大鍵Ｋ１～Ｋｎを生成する拡大鍵生成部１０と、拡大鍵生成部１０により生成された拡大鍵Ｋ１～Ｋｎを順次各ラウンドＲ１～Ｒｎに用いて暗号化又は復号を行う攪拌部２０とを備えている。すなわち、拡大鍵生成部１０及び攪拌部２０は、暗号化と復号に共通して用いられており、ソフトウェアにより暗復号装置を実現する場合には両者の動作を示すプログラムが予め記憶媒体からインストールされている。なお、拡大鍵生成部１０及び攪拌部２０との間には転置処理等を設けてもよい。

【００５０】

ここで、拡大鍵生成部１０は、各ラウンドＲ１～Ｒｎに対応し、順にカスケード接続された鍵変換関数ｆｋ１～ｆｋｎ（単に鍵変換関数ｆｋともいう）が設けられている。鍵変換関数ｆｋ１～ｆｋｎは、共通鍵ＫＣ若しくは中間的な鍵変換結果ｋｃ１～ｋｃn-1 が入力されると、これを変換して得られた拡大鍵Ｋ１～Ｋｎを攪拌部２０のラウンド関数ｆｒ１～ｆｒｎに出力し、また別途得られた中間的な鍵変換関数ｋｃ１～ｋｃn-1 を次段の鍵変換関数ｆｋ２～ｆｋｎに入力する機能をもっている。

【００５１】

ここで、鍵変換関数ｆｋ１～ｆｋｎは、図２に示すように、一時鍵レジスタ11_1～11_n、定数レジスタ12_1～12_n、ＸＯＲ素子13_1～13_n、Ｓボックス14_1～14_n、拡大変換部15_1～15_n、加算部16_1～16_n及び

巡回シフト部１７$_1$～１７$_{n-1}$を備えている。なお、最終段の巡回シフト部１７$_n$は、次段に鍵変換関数ｆｋ（ｎ+1）が無く、不要であるため、省略されている。

【００５２】

一時鍵レジスタ１１$_i$（但し、１≦ｉ≦ｎ、以下も同様）は、拡大鍵生成部１０に入力された共通鍵又は前段の鍵変換関数ｆｋ(i-1）から入力された中間的な鍵変換結果を保持するものであり、ここでは、５６ビットのレジスタが使用されている。

【００５３】

定数レジスタ１２$_i$は、鍵変換関数ｆｋｉの属するラウンド数に対応して定数が設定され、設定値がＸＯＲ素子１３$_i$から読出可能となっている。具体的には、定数レジスタ１２$_i$は、ラウンド数ｎ＝１６の例を図３（ａ）に示すように、拡大鍵Ｋ１～Ｋ１６を逆順（Ｋ１６～Ｋ１）にも生成可能な観点から、保持する定数がラウンド数の中央値（ｎ＝８，９）を中心として左右対称（前段，後段で対称）に設定されている。但し、これに限らず、定数レジスタ１２$_i$は、拡大鍵Ｋ１～Ｋ１６を逆順（Ｋ１６～Ｋ１）にも生成可能であれば、保持する定数は任意であり、例えば図３（ｂ）に示すように、暗号化と復号の時とで定数を置換しても良い。なお、定数レジスタ１２$_i$は、保持する定数のうち、少なくともどれか一つの値を他とは異ならせて設定されていれば良い。

【００５４】

ＸＯＲ素子１３$_i$は、一時鍵レジスタ１１$_i$内の８ビットのデータからなる第１鍵ＫＡと、定数レジスタ内の定数との排他的論理和を算出し、得られた８ビットの算出結果をＳボックスに入力するものである。

【００５５】

Ｓ（置換：substitution）ボックス１４$_i$は、弱鍵（全ての段で同じ拡大鍵）の生成を阻止するためのものであり、具体的には、ＸＯＲ素子１３$_i$から入力された８ビットの値を非線形変換し、得られた８ビットの変換結果を拡大変換部１５$_i$に入力する機能を有し、例えば図４に示すように入力ビットと出力ビットとを置換するための置換テーブルが使用可能となっている。例えば、Ｓボックス１

４ｉでは、入力ビットが（００００００００１）である場合、その（００００００００１）という情報を２進表現であるとみなし、さらにその２進表現を１０進表現した値「１」に変換する。

【００５６】

そして、図４の置換テーブルを参照して「１番目」の要素「５４」を決定し、その２進表現である（０１０１０１００）を出力ビットとして出力する。

そのため、入力ビット（００００００００１）を出力ビット（０１０１０１００）に置換することができる。

【００５７】

なお、上述のように図４の置換テーブルは０番～２５５番目までの２５６個の入力に対応した要素を保持しており、０～２５５の値が入力された場合に対応する０～２５５の値を決定する場合に用いられるものである。

【００５８】

また、Ｓボックス１４$_i$は、装置規模の縮小化の観点から、後述するラウンド関数ｆｋ内のいずれかのＳボックスと共有することが好ましい。

【００５９】

拡大変換部１５$_i$は、Ｓボックス１４$_i$から入力された８ビットの変換結果を大きな値に変換するものであり、ここでは、８ビットの変換結果を４ビットだけ左シフトさせるように拡大変換し、得られた１２ビットの拡大変換結果を加算部１６$_i$に入力する機能をもっている。

【００６０】

なお、拡大変換部１５$_i$のシフト量は、Ｓボックス１４$_i$の出力ビットを後述する攪拌部２０の２つのＳボックスＳ３，Ｓ４に反映させる観点から、等価的にＳボックス１４$_i$の出力ビット数（＝８）の半分（＝４ビット）とすることが好ましい。ここで、「等価的に」の語は、４ビットシフトに代えて、例えば１２（＝４＋８×１）ビットシフト又は２０（＝４＋８×２）ビットシフトのように、出力ビット数の整数倍を加えた変形例（換言すると、出力ビット数（＝８）で除算すると、余りが除数の半分（＝４）のビット数となるシフト量をもつ変形例）を包含することを意味している。また、Ｓボックス１４$_i$の出力ビットは、１２

ビットシフトされた場合には、ＳボックスＳ３，Ｓ４ではなく、ＳボックスＳ２，Ｓ３に反映され、２０ビットシフトされた場合にはＳボックスＳ１，Ｓ２に反映される。さらに、Ｓボックス１４$_i$の出力ビットを２つのＳボックスＳ３，Ｓ４（Ｓ２，Ｓ３又はＳ１，Ｓ２を含む）に反映させる場合、４ビットずつの組合せに限らず、順不同で１ビットと７ビット、２ビットと６ビットあるいは３ビットと５ビットの組合せとしてもよい。すなわち、等価的な４ビットシフトに代えて、等価的な１～３，５～７の任意のビットシフトとしてもよい。

【００６１】

加算部１６$_i$は、拡大変換部１５$_i$から入力された１２ビットの拡大変換結果と、一時鍵レジスタ１１$_i$内の３２ビットのデータからなる第２鍵ＫＢとを加算し（桁上りを伴う通常の加算）、得られた加算結果をラウンドＲｉの拡大鍵Ｋｉとして撹拌部２０のラウンド関数ｆｒｉに入力する機能をもっている。

【００６２】

なお、一時鍵レジスタ１１$_i$から抽出される第１鍵ＫＡ及び第２鍵ＫＢは、図２においては、それぞれ連続する領域から個別に取出されたが、これに限らず、不連続な領域から取り出してもよい。すなわち、第１鍵ＫＡは、一時鍵レジスタ１１$_i$内の任意の合計８ビットのデータであればよく、第２鍵ＫＢは、一時鍵レジスタ１１$_i$内の任意の合計３２ビットのデータであればよい。また、第１鍵ＫＡは、第２鍵ＫＢと重なっていてもよい。なお、第１鍵ＫＡのビット長は、撹拌部２０のＳボックスの入力ビット長と等しくすることがＳボックスの共有化の観点から好ましい。第２鍵ＫＢのビット長は、拡大鍵Ｋｉのビット長と等しくすることが、設計の簡易化の観点から好ましい（但し、所望により、第２鍵ＫＢと拡大鍵Ｋｉのビット長を互いに異ならせてもよく、この場合、例えば縮約型転置や拡大転置等を用い、最終的に拡大鍵Ｋｉのビット長を調整可能である）。

【００６３】

巡回シフト部１７$_i$は、一時鍵レジスタ１１$_i$の値を所定のシフト量だけ巡回シフトさせて次段の一時鍵レジスタ１１$_{i+1}$に入力するものであり、ここでは図５に示すように、各鍵変換関数ｆｋ１～ｆｋｎ毎に、シフト量が設定されている。なお、巡回シフト部１７$_i$のシフト量は、鍵の撹拌性を高める観点から、少な

くとも共通鍵ＫＣのビット数又はＳボックス１４$_i$の出力ビット数のいずれかと互いに素であることが好ましく、三者が互いに素であることが最も好ましい。また、このシフト量は、拡大鍵Ｋ１～Ｋ１６を逆順（Ｋ１６～Ｋ１）にも生成可能とする観点から、最終段を除いた鍵変換関数ｆｋ１～ｆｋ（ｎ+1）の中央値（ｎ＝８）を中心として左右対称（前段，後段で対称）に設定されている。但し、これに限らず、巡回シフト部１７$_i$は、拡大鍵Ｋ１～Ｋ１６を逆順（Ｋ１６～Ｋ１）にも生成可能であれば、シフト量及び巡回方向を任意に設定可能である。

【００６４】

一方、攪拌部２０は、夫々ラウンドＲ１からラウンドＲｎまでのｎラウンドの処理において、拡大鍵生成部１０から順に拡大鍵Ｋ１～Ｋ１６が与えられるとき、入力された平文を暗号化して暗号文を出力する暗号化機能を有し、また、拡大鍵生成部１０から暗号化とは逆順に拡大鍵Ｋ１６～Ｋ１が与えられるとき、入力された暗号文を復号して平文を出力する復号機能を有している。攪拌部２０には、各ラウンドＲ１～Ｒｎに対応して、順にカスケード接続されたラウンド関数ｆｒ１～ｆｒｎが設けられている。

【００６５】

ラウンド関数ｆｒｉは、暗号化のとき、平文又は中間的な暗号化結果を、拡大鍵生成部１０から入力された拡大鍵Ｋｉに基づいて変換し、中間的な暗号化結果又は暗号文を出力する関数であり、復号のとき、暗号文又は中間的な復号結果を、拡大鍵生成部１０から逆順に入力された拡大鍵Ｋ(n+1-i) に基づいて変換し、中間的な復号結果又は平文を出力する関数であって、ここでは一例として図６に示す如きFeistel 構造が使用されている。

【００６６】

図６中のFeistel 構造は、与えられた２つのサブブロックＬｉ，Ｒｉからなるデータブロックのうち、一方のサブブロックＲｉを拡大鍵Ｋｉに基づいてＦ関数で非線形変換し、この変換結果と他方のサブブロックＬｉとの排他的論理和をＸＯＲ素子２１で算出し、この算出結果Ｒi+1 と一方のサブブロックＬi+1 （＝Ｒｉ）との位置を交替して次段に与える、という構成を備えている。

【００６７】

ここで、Ｆ関数は、図６中において、拡大鍵Ｋとサブブロック Ｒｉ（又はＬｉ）との排他的論理和を算出するＸＯＲ素子２２と、ＸＯＲ素子２２の出力を４分割して夫々非線形変換する４つのＳボックスＳ１～Ｓ４とから構成される。

【００６８】

なお、各ラウンド関数ｆｒによる変換は、同じ変換を２回繰り返すと、元のデータが復元されるインボルーション（involution）という性質をもっている。このため、攪拌部２０では、平文を拡大鍵Ｋ１～Ｋ１６の順に変換して暗号文を生成したとき、この暗号文を拡大鍵Ｋ１６～Ｋ１の順に再度変換すると、平文が生成可能となっている。

【００６９】

次に、以上のように構成された暗復号装置の動作を説明する。

暗号化の際には、図１に示すように、入力された共通鍵ＫＣ又は中間的な鍵変換結果ｋｃｉは、鍵変換関数ｆｋｉにより１ラウンド毎に拡大鍵Ｋｉに変換される。

【００７０】

詳しくは図７に示すように、鍵変換関数ｆｋｉにおいては、一時鍵レジスタ１１$_i$から取り出した８ビットの第１鍵ＫＡと定数レジスタ１２$_i$内の定数との排他的論理和をＸＯＲ素子１３$_i$が算出し、この算出結果をＳボックス１４$_i$が非線形変換する。非線形変換としては、例えば図４に示した関係で入力と出力とを各ビット毎に置換する。この置換結果は、拡大変換部１５$_i$により４ビット左シフト（＝１６倍）されて加算部１６$_i$に入力される。

【００７１】

加算部１６$_i$は、入力されたシフト結果と一時鍵レジスタ１１$_i$から取り出した３２ビットの第２鍵ＫＢとを加算し、加算結果を３２ビットの拡大鍵Ｋｉとして攪拌部２０に出力する。

【００７２】

この拡大鍵Ｋｉにおいては、Ｓボックス１４$_i$で変換された８ビットの第１鍵ＫＡが、右（最下位桁）から５ビット目～１２ビット目に位置する。このビット位置は、第３及び第４のＳボックスＳ３，Ｓ４への入力に対応する。従って、拡

大鍵生成部１０のＳボックス１４$_i$による攪拌作用を攪拌部２０の２つのＳボックスＳ３，Ｓ４に反映でき、拡大鍵の攪拌性が向上されている。

【００７３】

また、攪拌部２０では、平文が、各ラウンド関数ｆｒ１～ｆｒｎ毎に各拡大鍵Ｋ１～Ｋｎに基づいて変換され、中間的な暗号化結果を経て最終的に暗号文に変換される。

【００７４】

一方、復号の際には、拡大鍵生成部１０においては、前述同様に共通鍵ＫＣが入力されると、暗号化時とは逆順に鍵変換処理が行われ、拡大鍵Ｋｎ～Ｋ１が順次、攪拌部２０に出力される。

【００７５】

攪拌部２０では、入力された暗号文が、暗号化時とは逆順の拡大鍵Ｋｎ～Ｋ１に基づいて変換され、中間的な復号結果を経て最終的に平文に変換される。

【００７６】

上述したように本実施形態によれば、各鍵変換関数ｆｋ１～ｆｋｎとしては、入力された鍵から得られた第１鍵ＫＡに基づいてＳボックス１４$_i$（置換テーブル）により変換処理を行い、加算部１６$_i$が、このＳボックス１４$_i$による変換結果を左シフトさせた値と、入力された鍵から得られた第２鍵ＫＢとに基づいて拡大鍵Ｋ１～Ｋ１６を算出する。

【００７７】

このように、外部装置を付加しない簡易な構成を用いており、拡大鍵Ｋｉを生成する際に、置換テーブル（Ｓボックス１４ｉ）による非線形変換処理を行うため、装置価格や装置規模を抑え、弱鍵の生成を阻止しつつ拡大鍵の攪拌性を向上でき、もって、暗号強度を向上させることができる。

【００７８】

また、各鍵変換関数ｆｋｉでは、巡回シフト部１７$_i$が、入力された鍵を左（又は右）に巡回シフトさせ、巡回シフトの完了した鍵を次ラウンドの鍵変換関数ｆｋ(i+1)に入力するので、容易且つ確実に、各ラウンドに入力される鍵を互いに相違させることができる。

【００７９】

さらに、巡回シフト部１７$_i$のシフト量としては、例えば、Ｓボックス１４$_i$の出力ビット数と互いに素な値とした場合、各ラウンドＲ１～Ｒｎにおけるほぼ全ての第１鍵ＫＡを互いに相違させることができ、前述した効果をより一層、容易且つ確実に得ることができる。

【００８０】

さらに、各鍵変換関数ｆｋｉとしては、拡大変換部１５$_i$が、Ｓボックス１４$_i$による変換結果を拡大変換させて加算部１６$_i$に入力するので、前述した効果に加え、第１鍵ＫＡの攪拌作用を拡大鍵Ｋｉの任意の領域に反映させることができる。

【００８１】

また、拡大変換部１５$_i$による拡大変換としては、所定ビット数のシフトであるので、前述した効果を容易且つ確実に得ることができる。

【００８２】

さらに、攪拌部２０が、暗号化及び復号のための複数のＳボックスＳ１～Ｓ４を有し、攪拌部２０のいずれかのＳボックスが、鍵変換関数ｆｋ１～ｆｋｎのＳボックス１４$_i$と共有化されているので、装置規模の縮小化を図ることができる。

【００８３】

また、各鍵変換関数ｆｋ１～ｆｋｎとしては、拡大変換部１５$_i$が、Ｓボックス１４$_i$による変換結果を受けたとき、この変換結果のビット数の半分のビット数、あるいは半分のビット数に変換結果のビット数の整数倍を加えた値のビット数だけ、当該変換結果を左シフトさせて加算部１６$_i$に入力するので、第１鍵ＫＡの攪拌作用を拡大鍵Ｋｉにて左シフトさせた領域に反映させることができ、この場合、攪拌部２０の複数のＳボックスＳ３，Ｓ４に入力される領域に反映させることができるので、より一層、暗号強度の向上を図ることができる。

【００８４】

（第２の実施形態）

図８は本発明の第２の実施形態に係る拡大鍵生成装置に適用される鍵変換関数

の構成を示すブロック図であり、図２と同一部分には同一符号を付してその詳しい説明を省略し、ここでは異なる部分についてのみ述べる。なお、以下の各実施形態も同様にして重複した説明を省略する。

【００８５】

すなわち、本実施形態は、第１の実施形態の変形例であり、拡大鍵の攪拌性のより一層の向上を図るものであり、具体的には図２に示すように、各鍵変換関数において、前述した定数レジスタ１２$_i$、ＸＯＲ素子１３$_i$、Ｓボックス１４$_i$及び拡大変換部１５$_i$からなる変換要素が互いに並列に、一時鍵レジスタ１１$_i$と加算部１６$_i$との間に接続されている。

【００８６】

ここで、２つのＳボックス１４$_i$は、１種類で設けてもよく、又は複数の種類で設けてもよいが、複数の種類を用いる場合、共通鍵ＫＣに基づいて拡大鍵Ｋｉを正順及び逆順の両方で生成可能とする観点から、前半の鍵変換関数ｆｋ１～ｆｋ８と後半の鍵変換関数ｆｋ９～ｆｋ１６とでは中央（ｆｋ８，９）から上下対称となるように種類が設けられることが好ましい。

【００８７】

また、２つの拡大変換部１５ｉは、互いに同一のシフト量とすることも可能であるが、２つのＳボックス１４$_i$による攪拌効果をより広範囲に反映させる観点から、互いに異なるシフト量でＳボックス１４$_i$の出力を左シフトさせることが好ましい。この場合、例えば一方の拡大変換部１５$_i$を４ビットの左シフトとし、他方の拡大変換部１５$_i$を２０ビットの左シフトとすると、第１鍵ＫＡの攪拌効果を攪拌部２０のＳボックスＳ１～Ｓ４の全てに反映できるので好ましい。

【００８８】

以上のような構成によれば、第１鍵ＫＡによる攪拌性をさらに向上できるので、第１の実施形態の効果に加え、拡大鍵Ｋｉの攪拌性をより一層向上させることができる。

【００８９】

（第３の実施形態）

図９は本発明の第３の実施形態に係る拡大鍵生成装置の構成を示すブロック図

である。

本実施形態は、第１又は第２の実施形態の変形形態であり、一時鍵レジスタ１１$_i$及び巡回シフト部１７$_i$に代えて、入力される共通鍵ＫＣ又は中間的な鍵ｋｃ１～ｋｃn-1 の各ビットを互いに非線形的に置換し、得られた中間的な鍵の一部を自己の段のＸＯＲ素子１３$_i$並びに加算部１６$_i$に入力すると共に、その中間的な鍵の全体を次段の置換処理部１８$_{(i+1)}$ に入力する置換処理部１８$_i$を備えている。

【００９０】

各置換処理部１８$_i$は、共通鍵ＫＣに基づいて拡大鍵Ｋｉを正順及び逆順の両方で生成可能とする観点から、共通鍵ＫＣを正順にｎ回置換した結果が元の共通鍵ＫＣに等しくなるように夫々設定され、且つラウンド数ｎ＝１６の場合の例を図１０に示すように、暗号化の際には昇順に変換を行い、復号の際には降順に逆変換を行うように設定されている。

【００９１】

以上のような構成としても、第１又は第２の実施形態と同様の効果を得ることができ、これに加え、容易且つ確実に、各鍵変換関数ｆｋ１～ｆｋｎに入力される鍵ＫＣ，ｋｃ１～ＫＣn-1 を互いに相違させることができる。

【００９２】

なお、上記各実施形態では、Ｓボックス１４$_i$の入力側に、定数を排他的論理和するＸＯＲ素子１３$_i$を設けた場合について説明したが、これに限らず、ＸＯＲ素子１３$_i$を省略し、Ｓボックス１４$_i$に代えて、定数の排他的論理和を算出した後のＳボックス１４ｘ$_i$を設けた構成としても、本発明を同様に実施して同様の効果を得ることができる。

【００９３】

（第４の実施形態）

次に、本発明の第４の実施形態に係る暗復号装置について図１１を用いて説明する。この暗復号装置３０は、第１乃至第３の実施形態のいずれかで述べた構成を有し、例えば画像データや音楽データ等のディジタル情報（以下、生データという）を保護するためのものである。

【００９４】

係る暗復号装置３０は、例えば図１１に示すように、記憶媒体からプログラムがインストールされることにより、パーソナルコンピュータ（以下、パソコンという）ＰＣに実現されているとする。ここで、暗復号装置３０は、例えばユーザＩＤを共通鍵とし、パソコンＰＣに入力された生データを暗号化し、得られた暗号化データ（前述した暗号文に相当）を携帯可能な記憶素子３１に記憶させる。この種の記憶素子３１としては、ＩＣカード、スマートメディア又はメモリカードなどがある。

【００９５】

この記憶素子３１がユーザ宅へ配布され、ユーザ宅内の図示しない暗復号装置は、自己のユーザＩＤに基づいて記憶素子３１内の暗号化データを復号し、得られた画像データや音楽データをスピーカ等から再生出力させる。これにより、例えば予め契約したユーザのみに生データ（コンテンツ）を配布することができる。

【００９６】

また、本実施形態は、以下のように種々変形可能となっている。例えば、図１２に示すように、パソコンＰＣに代えて、例えばハードウェア回路からなる暗復号装置３０を備えた記録装置３２を設けた構成である。この構成によれば、コンテンツを記憶素子３１に書込む際に、暗復号装置３０がユーザＩＤ等により生データを暗号化して記憶素子３１に記憶させる。宅配から復号に至る過程は、前述した通りである。このように、パソコンＰＣ等の汎用のコンピュータでなくとも、専用の記録装置３２に暗復号装置３０を設けた構成としてもよい。

【００９７】

また、図１３に示すように、暗復号装置３０を設けたホストコンピュータ３３が、ネットワークＮＷを介してパソコンＰＣに接続された構成としてもよい。この場合、ホストコンピュータ３３からダウンロードされた暗号化データがパソコンＰＣを介して暗号化された状態で記憶素子３２に記憶される。宅配から復号に至る過程は、前述した通りである。この変形例によれば、前述した効果に加え、ネットワークＮＷ上でのコンテンツ（生データ）の盗聴などを防止することがで

きる。

【００９８】

さらに、図１４（ａ），（ｂ）に示すように、記憶素子を例えばＤＶＤ（digital versatile disc）としてもよい。図１４（ａ）に示す場合、予め暗号化データが格納されたＤＶＤ３４がユーザに頒布される。ユーザ宅の暗復号装置３０は、ＤＶＤ３４内の暗号化データを復号し、得られた画像データや音楽データをスピーカ等から再生出力させる。

【００９９】

また、図１４（ｂ）に示す場合、画像や音楽等の生データがユーザ宅の暗復号装置３０によって所定の共通鍵を用いて暗号化され、得られた暗号化データがＤＶＤ－ＲＡＭ３５に格納される。

この暗号化データは、ユーザにより設定された所定の共通鍵により復号されるが、共通鍵が知られない限り、他人には復号されない。従って、趣味的な画像データや音楽データなどを他人から保護しつつ保存することができる。

【０１００】

（他の実施形態）

尚、本発明における拡大鍵生成装置及び暗復号装置の処理を実現させるためのプログラムが記憶された記憶媒体としては、磁気ディスク、フロッピーディスク、ハードディスク、光ディスク（ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ等）、光磁気ディスク（ＭＯ等）、半導体メモリ等が適用可能である。実際には、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【０１０１】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行しても良い。

【０１０２】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、

ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【０１０３】

また、記憶媒体は１つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【０１０４】

尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【０１０５】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【０１０６】

また、本発明は、ＤＥＳ暗号系に限らず、ラウンド関数を用いるブロック暗号系であれば適用可能であり、例えば、Lucifer 、LOKI、MISTY 1 、MISTY 2 及びSAFER(Secure And Fast Encryption Routine) といった暗号系に適用してもよい。

【０１０７】

その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【０１０８】

【発明の効果】

以上説明したように本発明によれば、装置価格や装置規模を抑え、弱鍵の生成を阻止しつつ拡大鍵の攪拌性を向上でき、もって、暗号強度を向上できる拡大鍵生成装置、暗復号装置及び記憶媒体を提供できる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態に係る暗復号装置の構成を示すブロック図

【図２】

同実施形態における暗復号装置内の拡大鍵生成部の構成を示すブロック図

【図３】

同実施形態における定数レジスタの設定値を説明するための模式図

【図４】

同実施形態におけるＳボックスの構成を説明するための模式図

【図５】

同実施形態における巡回シフト部の設定を説明するための模式図

【図６】

同実施形態におけるラウンド関数の構造を示すブロック図

【図７】

同実施形態における動作を説明するための模式図

【図８】

本発明の第２の実施形態に係る拡大鍵生成装置に適用される鍵変換関数の構成を示すブロック図

【図９】

本発明の第３の実施形態に係る拡大鍵生成装置の構成を示すブロック図

【図１０】

同実施形態における置換処理部の設定を説明するための模式図

【図１１】

本発明の第４の実施形態に係る暗復号装置を説明するための模式図

【図１２】

同実施形態における変形例を説明するための模式図

【図１３】

同実施形態における変形例を説明するための模式図

【図１４】

同実施形態における変形例を説明するための模式図

【図１５】

従来の共通鍵暗号の一例としてのＤＥＳ方式を説明するためのブロック図

【符号の説明】

１０…拡大鍵生成部

１１_{1}～１１_{n}…一時鍵レジスタ

１２_{1}～１２_{n}…定数レジスタ

１３_{1}～１３_{n}…ＸＯＲ素子

１４_{1}～１４_{n}…Ｓボックス

１５_{1}～１５_{n}…拡大変換部

１６_{1}～１６_{n}…加算部

１７_{1}～１７_{n-1}…巡回シフト部

１８_{i}…置換処理部

２０…攪拌部

３０…暗復号装置

３１…記憶素子

３２…記録装置

３３…ホストコンピュータ

３４…ＤＶＤ

３５…ＤＶＤ－ＲＡＭ

ｆｋ１～ｆｋｎ…鍵変換関数

Ｒ１～Ｒｎ…ラウンド

Ｋ１～Ｋｎ…拡大鍵

ＫＣ…共通鍵

ｋｃ１～ｋｃn-1 …鍵変換結果

ＫＡ…第１鍵

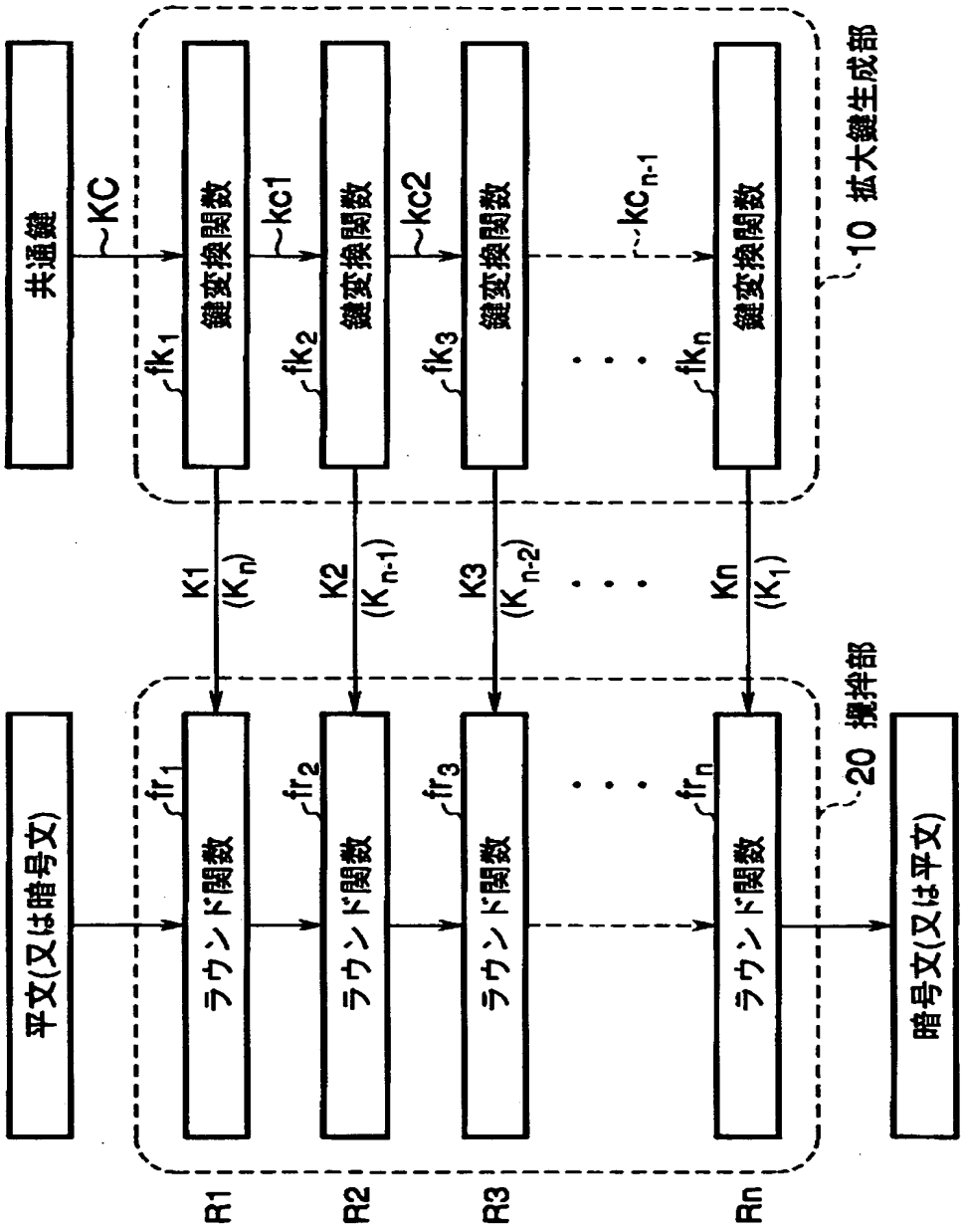
ＫＢ…第２鍵

ＰＣ…パソコン

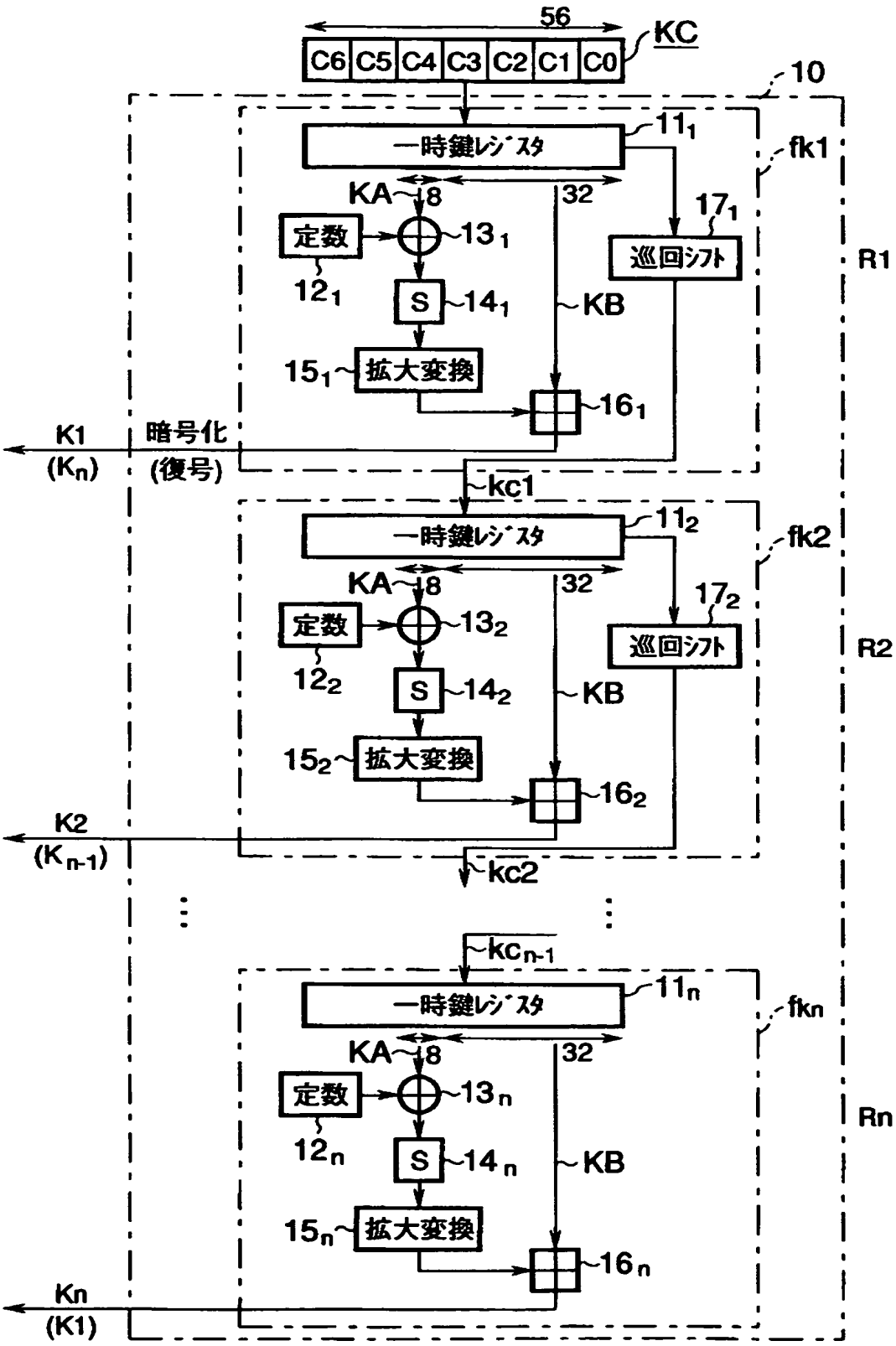
ＮＷ…ネットワーク

【書類名】　　図面

【図１】

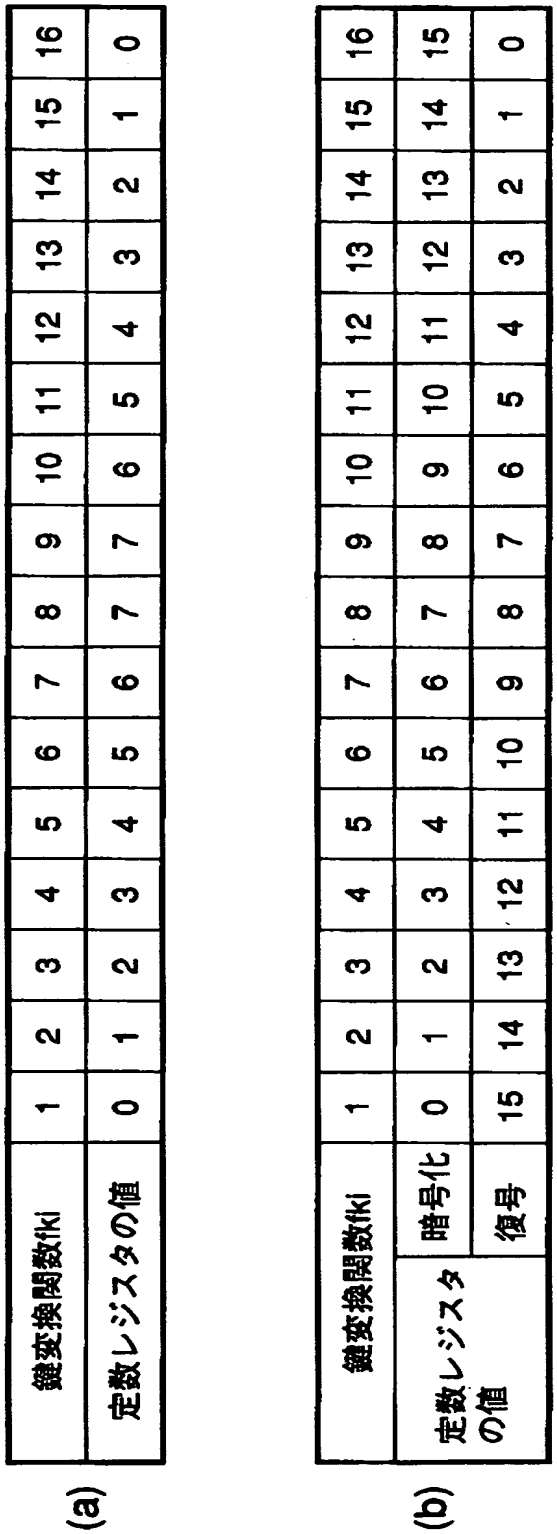

共通鍵
KC
鍵変換関数
fk1
kc1
fk2
kc2
fk3
kcn-1
fkn
10 拡大鍵生成部
K1 (Kn)
K2 (Kn-1)
K3 (Kn-2)
Kn (K1)
平文(又は暗号文)
ラウンド関数
fr1
fr2
fr3
frn
20 攪拌部
暗号文(又は平文)
R1
R2
R3
Rn

【図２】



出証特２０００－３０５１６２８

【図３】



(a)

鍵変換関数fki	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
定数レジスタの値	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	0

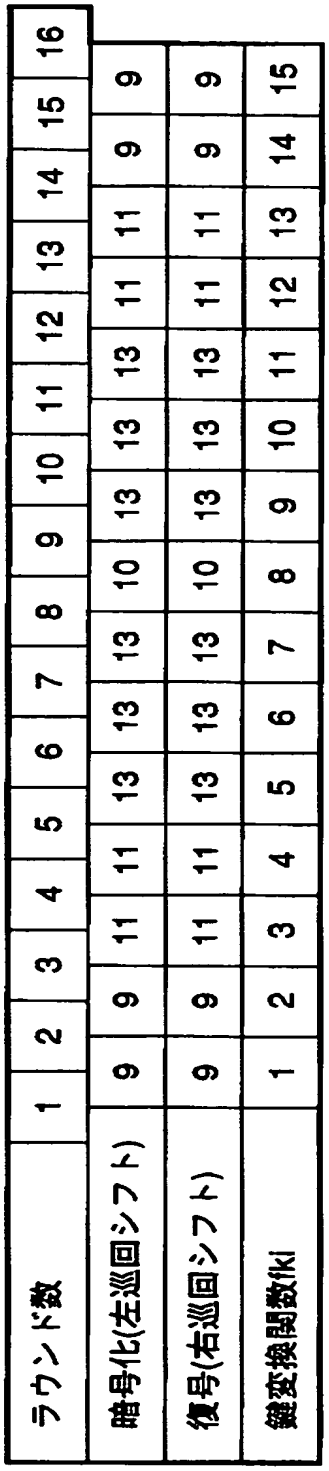
(b)

鍵変換関数fki		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
定数レジスタの値	暗号化	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	復号	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

【図４】

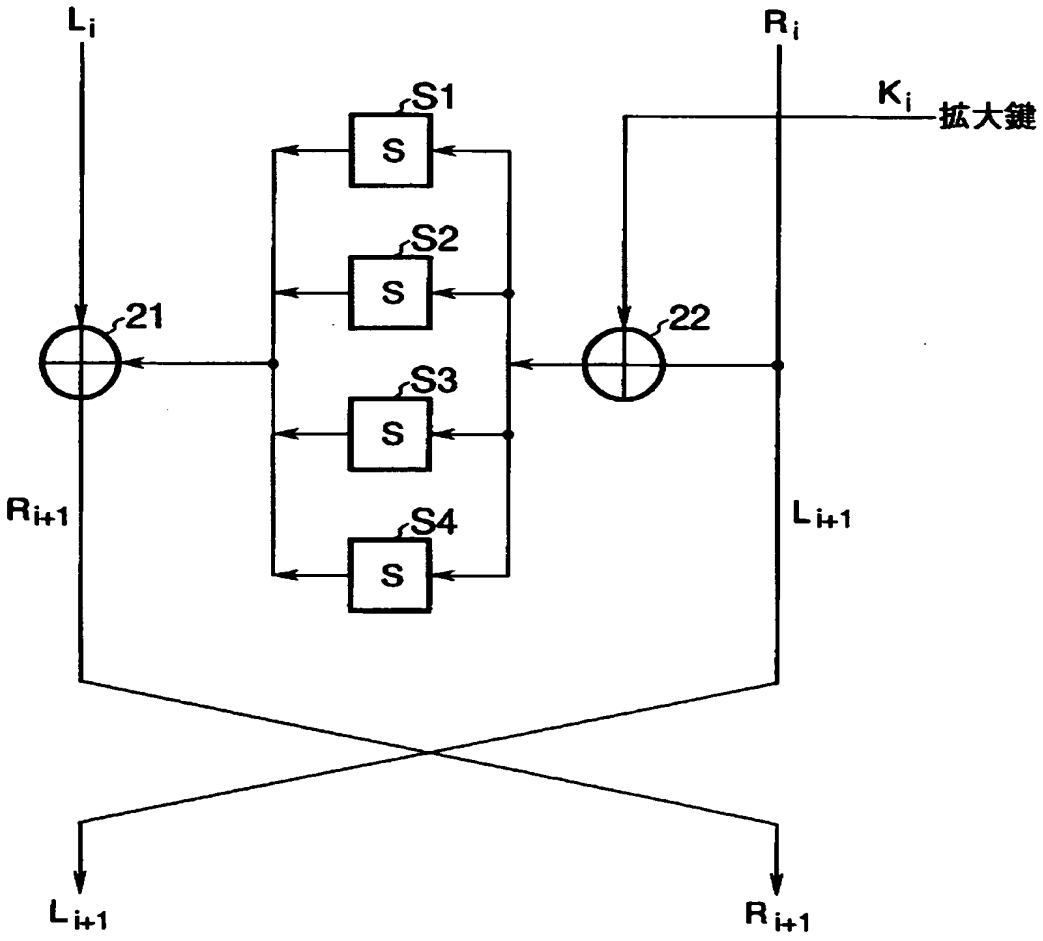
48,	54,	216,	182,	175,	5,	130,	229,	107,	52,	86,	11,	12,	221,	14,	15,
59,	4,	41,	140,	22,	164,	7,	89,	124,	81,	225,	176,	101,	66,	30,	118,
126,	242,	44,	211,	18,	161,	249,	105,	222,	174,	141,	202,	34,	103,	87,	233,
71,	49,	187,	51,	39,	1,	91,	77,	181,	172,	55,	42,	199,	79,	62,	194,
64,	72,	68,	133,	190,	158,	165,	232,	231,	115,	186,	116,	217,	240,	129,	171,
74,	169,	204,	173,	57,	58,	93,	17,	159,	245,	241,	155,	92,	156,	94,	26,
132,	82,	109,	230,	227,	28,	131,	209,	170,	25,	106,	73,	85,	98,	128,	143,
237,	108,	160,	61,	21,	179,	254,	197,	38,	122,	235,	70,	125,	31,	40,	102,
246,	119,	207,	53,	214,	111,	63,	135,	184,	236,	138,	56,	19,	29,	213,	88,
144,	145,	243,	127,	148,	137,	189,	151,	78,	153,	123,	183,	114,	157,	255,	252,
33,	6,	147,	163,	84,	97,	166,	167,	192,	0,	10,	208,	117,	196,	9,	16,
27,	206,	177,	104,	195,	83,	24,	75,	150,	203,	188,	50,	100,	69,	20,	180,
134,	193,	168,	8,	251,	247,	149,	201,	200,	112,	43,	142,	139,	205,	212,	37,
60,	226,	210,	154,	239,	80,	244,	215,	3,	120,	45,	23,	67,	99,	219,	223,
250,	220,	191,	32,	185,	253,	121,	13,	36,	228,	96,	162,	136,	46,	238,	146,
110,	178,	152,	2,	90,	234,	95,	65,	248,	113,	224,	35,	76,	218,	198,	47,

【図５】

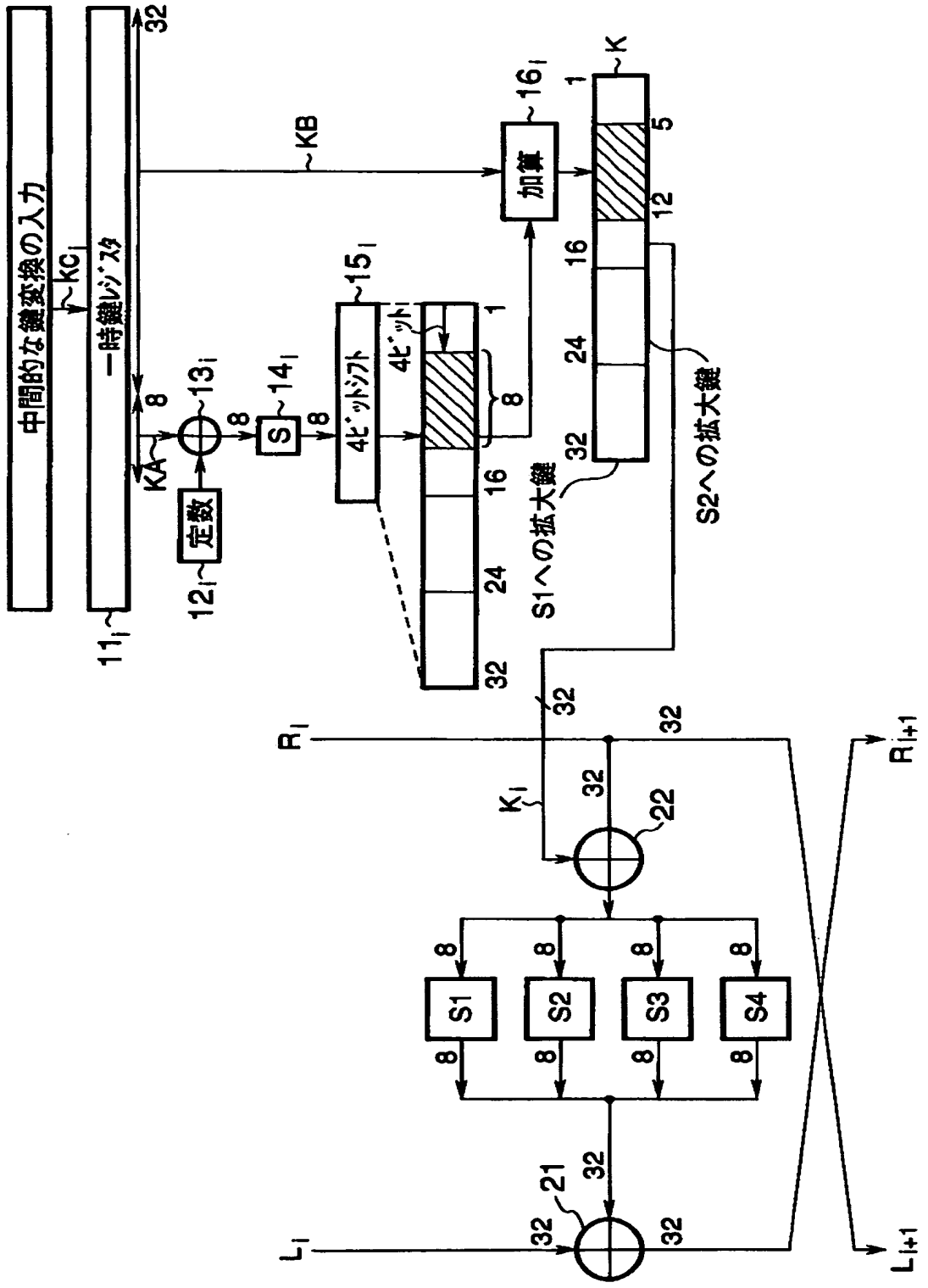


ラウンド数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
暗号化(左巡回シフト)	9	9	11	11	13	13	13	10	13	13	13	11	11	9	9	
復号(右巡回シフト)	9	9	11	11	13	13	13	10	13	13	13	11	11	9	9	
鍵変換関数fkl	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	

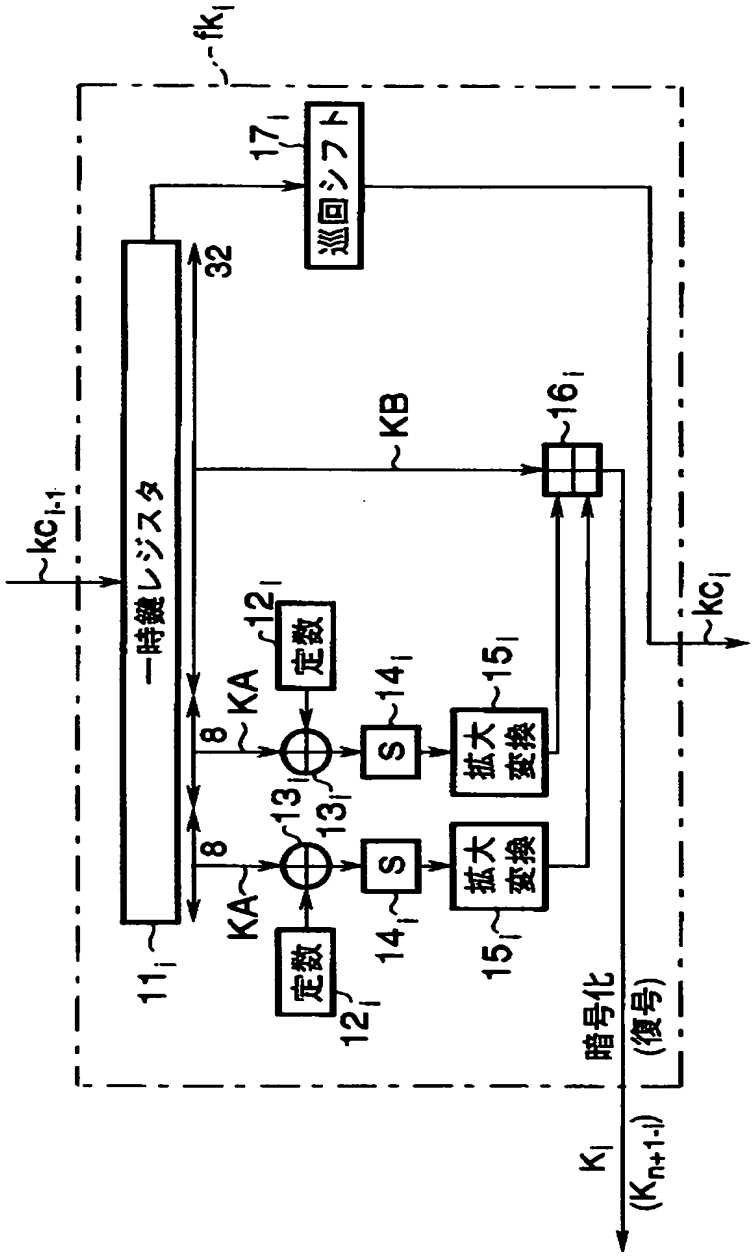
【図６】



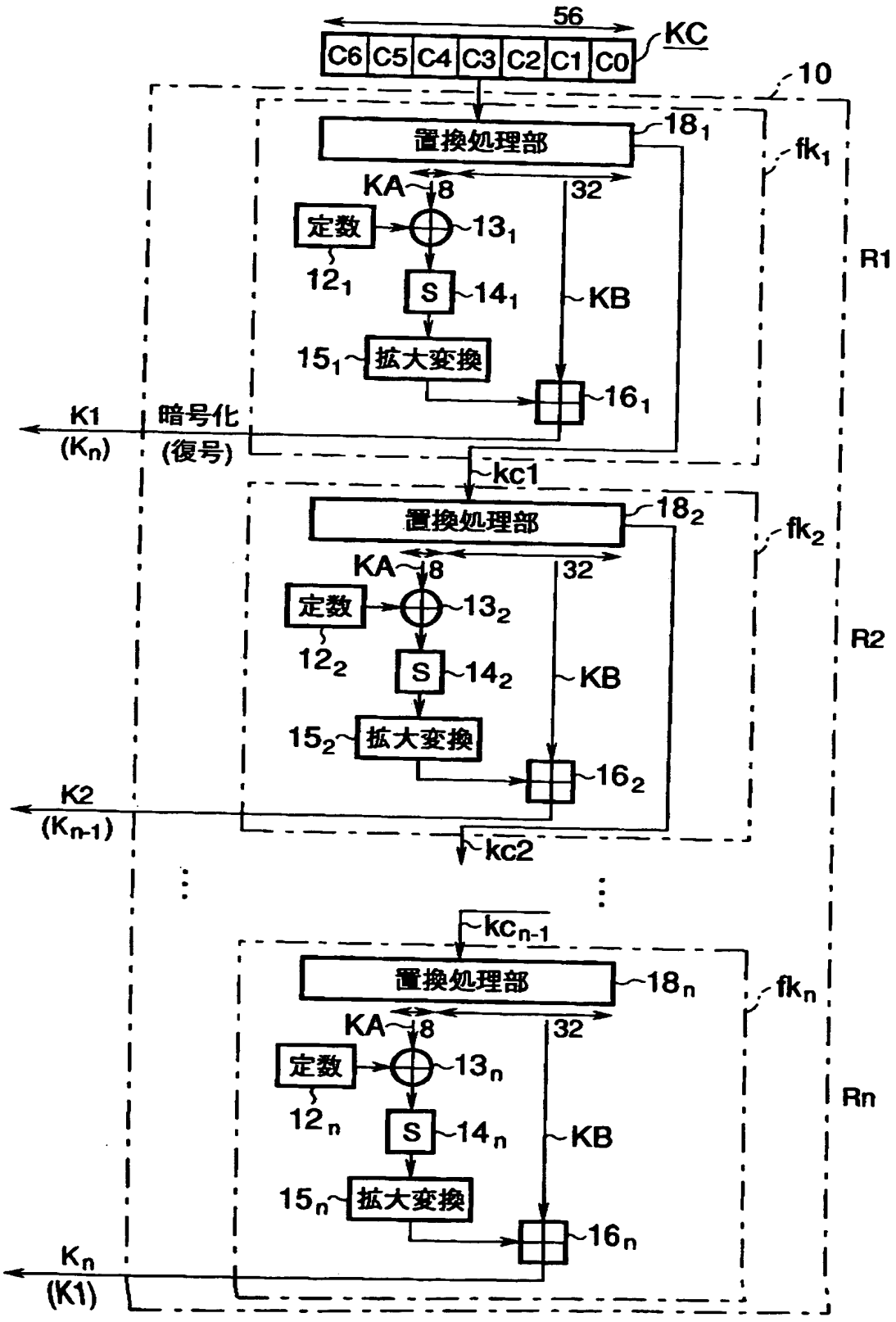
【図７】


中間的な鍵変換の入力
一時鍵レジスタ
KC$_i$
11$_i$
32
KB
16$_i$
加算
K
1
5
12
16
24
32
S1への拡大鍵
S2への拡大鍵
15$_i$
4ビットシフト
4ビット
1
8
16
24
32
13$_i$
14$_i$
S
KA
8
定数
12$_i$
R$_i$
K$_i$
22
S1
S2
S3
S4
21
L$_i$
R$_{i+1}$
L$_{i+1}$

【図８】


fk$_i$
17$_i$
巡回シフト
32
KB
16$_i$
kc$_{i-1}$
一時鍵レジスタ
kc$_i$
12$_i$
定数
KA
8
14$_i$
S
15$_i$
拡大変換
13$_i$
13$_i$
8
KA
S
拡大変換
11$_i$
14$_i$
15$_i$
定数
12$_i$
暗号化
(復号)
K$_i$
(K$_{n+1-i}$)

【図９】

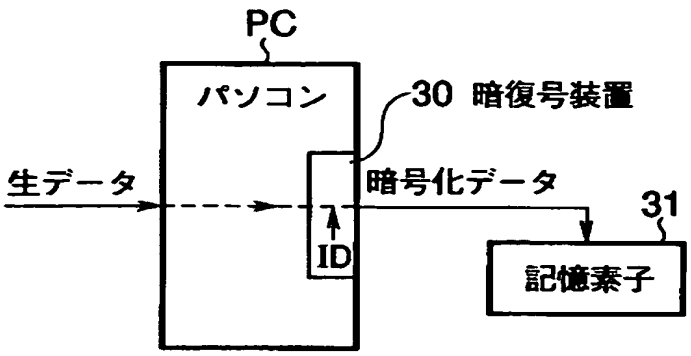


出証特２０００－３０５１６２８

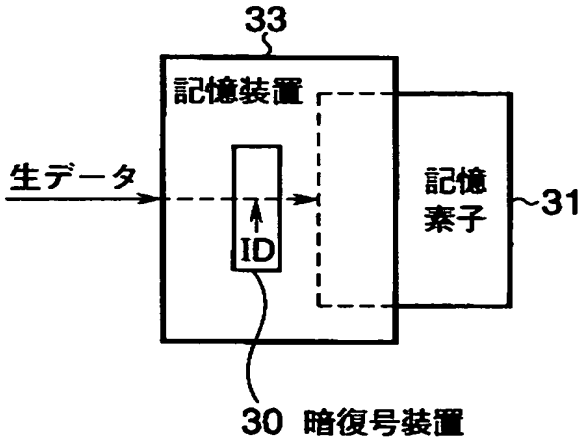
【図１０】

ラウンド数		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
転置入力処理	暗号化	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16
	復号	$P16^{-1}$	$P15^{-1}$	$P14^{-1}$	$P13^{-1}$	$P12^{-1}$	$P11^{-1}$	$P10^{-1}$	$P9^{-1}$	$P8^{-1}$	$P7^{-1}$	$P6^{-1}$	$P5^{-1}$	$P4^{-1}$	$P3^{-1}$	$P2^{-1}$	$P1^{-1}$

【図１１】

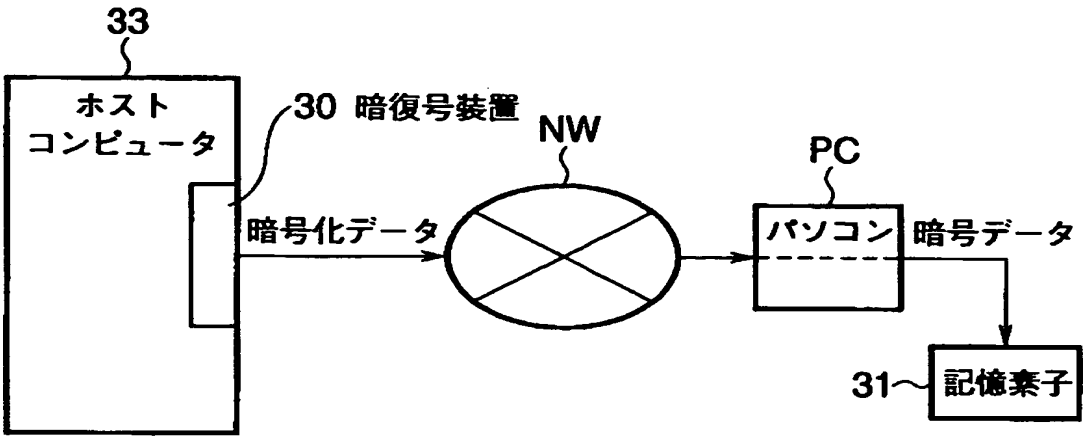


【図１２】

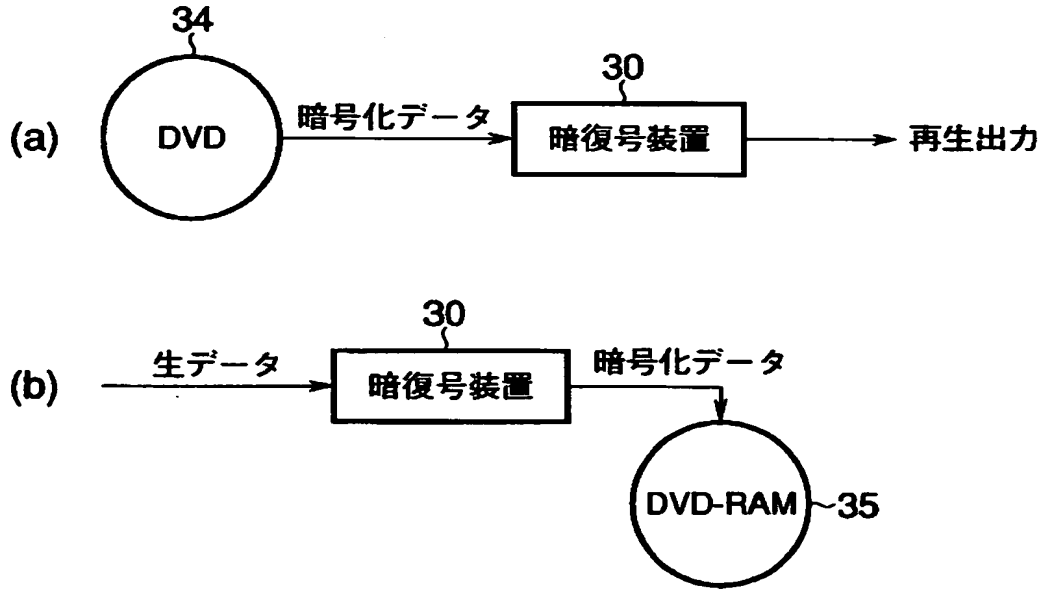


出証特２０００－３０５１６２８

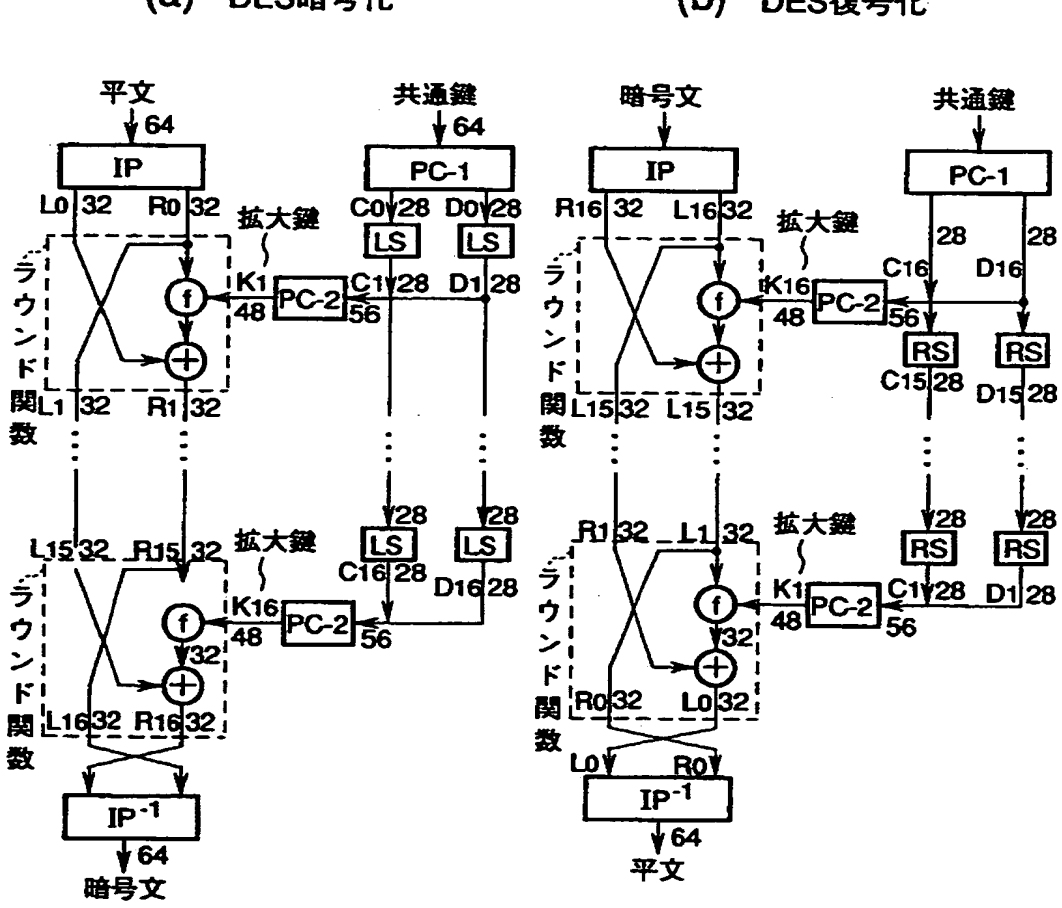
【図１３】


33
ホスト
コンピュータ
30 暗復号装置
NW
PC
暗号化データ
パソコン
暗号データ
31
記憶素子

【図１４】


34
(a)
DVD
暗号化データ
30
暗復号装置
再生出力
30
(b)
生データ
暗復号装置
暗号化データ
DVD-RAM
35

【図１５】


(a) DES暗号化
(b) DES復号化
平文
64
IP
L0 32 R0 32
拡大鍵
ラウンド関数
K1 48
PC-2
56
共通鍵
64
PC-1
C0 28 D0 28
LS
C1 28 D1 28
L1 32 R1 32
L15 32 R15 32
K16 48
C16 28 D16 28
32
L16 32 R16 32
IP-1
64
暗号文
暗号文
R16 32 L16 32
L15 32 L15 32
RS
C16 28 D16 28
C15 28 D15 28
R1 32 L1 32
R0 32 L0 32
L0 R0

【書類名】　　要約書

【要約】

【課題】　本発明は、装置価格や装置規模を抑え、弱鍵の生成を阻止しつつ拡大鍵の攪拌性を向上でき、もって、暗号強度の向上を図る。

【解決手段】　各鍵変換関数ｆｋ１～ｆｋｎとしては、入力された鍵から得られた第１鍵ＫＡに基づいてＳボックス１４$_i$（置換テーブル）により変換処理を行い、加算部１６$_i$が、このＳボックス１４$_i$による変換結果を左シフトさせた値と、入力された鍵から得られた第２鍵ＫＢとに基づいて拡大鍵Ｋ１～Ｋ１６を算出する拡大鍵生成装置、暗復号装置及び記憶媒体。

【選択図】　　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝

US 0965215703P1

Creation date: 06-29-2004
Indexing Officer: DGREEN - DONALD GREEN
Team: OIPEBackFileIndexing
Dossier: 09652157

Legal Date: 10-12-2000

No.	Doccode	Number of pages
1	CTMS	1

Total number of pages: 1

Remarks:

Order of re-scan issued on .....